CENTER FOR CYBERSIKKERHED

Vejledning

Råd om sikkerhed på virtuelle mødeplatforme

Gør det virtuelle møde mere sikkert.

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. udgave januar 2021.

Indledning

De fleste organisationer har længe benyttet sig af virtuelle mødeplatforme. Restriktionerne i forbindelse med Covid-19 og begrænsningen af fysiske møder har imidlertid medført en stor stigning i behovet for at mødes virtuelt. Og derfor også et øget behov for at sætte fokus på sikkerhed på virtuelle platforme.

Med begrebet *virtuelle mødeplatforme* menes der i denne publikation tjenester, der giver medarbejdere mulighed for at kommunikere via internettet med tekst (chat), tale og video samt deling af filer. Det kan være mellem to personer eller en stor gruppe.

Virtuelle mødeplatforme er reelt åbne fora – og bør betragtes som sådan i organisationens risikoarbejde, politikker og retningslinjer.

Denne vejledning adresserer nogle af de sikkerhedsmæssige problemstillinger, som særligt risiko-ledelsen og it-ledelsen bør forholde sig til, når der skal anskaffes og konfigureres virtuelle mødeplatforme.

Vejledningen er opdelt i to afsnit. Det ene handler om indstilling og konfiguration af mødeplatformen på en sikker måde. Det andet behandler de vurderingskriterier, der bør overvejes i forbindelse med valg af platform.

For hvert råd benyttes tre niveauer for sikkerhed: ”God”, ”Bedre” og ”Bedst”. Afhængig af situationen og det ønskede sikkerhedsniveau kan organisationen vælge enten ét af de tre niveauer eller en kombination af dem.

Det er vigtigt at påpege, at listen over råd ikke er en facitliste, da ikke alle platforme har samme funktionalitet eller teknologi. Rådene er heller ikke statiske, idet det samlede risikobillede løbende ændres i takt med, at teknologier udvikles, nye angrebsteknikker opstår, og nye sårbarheder identificeres. Ud over de råd, der er givet her, bør organisationen derfor altid overveje, hvilke yderligere tiltag, der er relevante. Det kan f.eks. være særlige adfærds- og spilleregler for brugen af disse platforme.

Ikke alle sikkerhedsmæssige aspekter vedrørende virtuelle mødeplatforme kan løses teknisk med opsætning og konfiguration. Teknikken bør, så vidt muligt, understøtte medarbejderen i at træffe de sikre og rigtige valg, hvad sikkerhed angår.

Indstilling og konfiguration

Center for Cybersikkerhed anbefaler, at organisationen vælger én eller to platforme, som indlejres i organisationens portefølje af it-arbejdsredskaber, og at det gøres til en del af organisationens politik, at disse altid bruges i forbindelse med virtuelle møder i organisationen.

Herunder gives en række råd til, hvordan organisationen bør indstille og konfigurere de(n) virtuelle mødeplatform(e), man vælger at anskaffe.

Råd 1. Brugeradministration (bruger fra egen organisation)
Sørg for at have styr på brugerne. Oprettelse og nedlæggelse af brugere bør kunne integreres med og styres fra organisationens eksisterende brugerstyringssystem, eksempelvis Active Directory, AD. Herved sikres en enkel brugeradministration, og man minimerer sandsynligheden for adgang fra uautoriserede brugere, f.eks. tidligere ansatte.

Er der ikke mulighed for integration med fx AD'et, anbefales en løsning, hvor nogle få privilegerede brugere tildeles rettigheder til at oprette og nedlægge brugere samt styre brugerrettigheder på platformen.

Hvilke muligheder, organisationen har, hænger ofte sammen med typen af licens, der vælges til mødeplatformen.

A: God	B: Bedre	C: Bedst
Separat, men granulær brugerstyring[1] fordelt på roller således, at det er muligt at have nogle få privilegerede brugere, der står for administration og tildeling af rettigheder på platformen.	Integration med eksisterende brugerstyring så eksisterende procedurer for brugeroprettelse og nedlæggelse kan benyttes.	Tæt integration så rettigheder kan styres og tildeles via roller og grupper i organisationens egen brugerstyrings system.

[1] Med granulær brugerstyring menes at systemrettigheder tildeles på en måde, hvorpå der kan konstrueres specifikke roller med privilegier, der passer til virksomhedens krav og som, hvor muligt, begrænser systemadministratorer fra at få adgang til brugerdata.

Råd 2. Brugeradministration (gæstebrugere)
Ved gæstebrugere menes eksterne brugere og mødedeltagere, der ikke har en brugerprofil og ikke administreres af organisationen selv. Disse eksterne mødedeltagere håndteres ofte af de virtuelle mødeplatforme ved, at der genereres og sendes et mødelink, som giver gæstebrugeren adgang til det pågældende møde.

Afhængig af den virtuelle mødeplatform har gæstebrugere ofte kun adgang til et begrænset sæt rettigheder og funktioner ved møder. Såfremt mødeplatformen giver mulighed for ændre på indstillinger for gruppen af gæstebrugere, anbefales det at begrænse deres rettigheder og funktioner til det nødvendige.

A: God	B: Bedre	C: Bedst
Begræns gæstebrugeres rettigheder og funktioner i mødet til det nødvendige.	Sørg for at gæstebrugere tildeles unikke mødelinks.	Sørg for ekstra validering af gæstebrugere fx med kode og at kode til mødedeltagelse sendes til disse umiddelbart før mødestart.

Råd 3. Fler-faktor validering
Det er en vigtig sikkerhedsmæssig styrke, at mødeplatformen understøtter fler-faktor login, når brugere tilgår den. Eksempelvis når en bruger logger ind på platformen fra en ukendt enhed, der ikke er kontrolleret af organisationen. Det kan være en privat computer, tablet eller smartphone.

Hvis ikke brugeradministration til platformen kan integreres med virksomhedens eksisterende brugerstyringssystem, bør det være muligt at opsætte politikker for passwordlængde og brug af fler-faktor validering.

A: God	B: Bedre	C: Bedst
Fler-faktor validering understøttes. Muligt at konfigurere politikker for password.	Integration med eksisterende brugerstyring og tvungen brug af fler-faktor ved adgang med enheder, der ikke er kendt af organisationen.	Integration med eksisterende brugerstyring og tvungen brug af fler-faktor fra alle typer enheder.

Råd 4. Styring af standardindstillinger i forbindelse med møder
Jo bedre den virtuelle platform understøtter muligheden for at definere sikre standardindstillinger, jo nemmere er det for brugeren at efterleve, og jo sikrere bliver mødeafholdelsen.

Vær opmærksom på, hvad mødeplatformen stiller til rådighed:

- Hvad kan indstilles som standard/minimumsindstillinger for oprettelse af møde?
- Er det muligt at definere, at der genereres unikke møde-links? Og er det muligt at brugeren skal taste unikke passwords, så genbrug kan undgås?
- Kan passwords sendes ad andre kanaler end mødelinket?

Center for Cybersikkerhed anbefaler, at alle møder har et unikt møde-link, og at organisationen undgår genbrug af mødelinks.

A: God	B: Bedre	C: Bedst
Brug unikke password til alle møder.	Brug unikt link til mødet, brug unikt password til mødet.	Brug unikt link til mødet, unikt password for hver enkelt deltager. Undgå så vidt muligt, at sende password ad samme kanal som mødelinket. Send passwords til deltagere kort før mødets start.

Råd 5. Styring af adgang og deltagelse i møder
Nogle platforme giver mulighed for, at deltagere først kommer ind i en lobby, inden de lukkes ind i selve mødet. Det giver mulighed for verificering af, hvem deltagerne er og kan forhindre, at uvedkommende forstyrrer mødet. Hvis en deltager kommer for sent, må de vente i lobbyen, til mødeværten lukker dem ind.

Ofte giver "lobbyfunktionen" også mulighed for at ekskludere deltagere, når de ikke længere har behov for at deltage. For eksempel behøver en (ekstern) oplægsholder, der skal give en præsentation, ikke at deltage i hele mødet.

Uanset om muligheden for lobby er til stede, er det altid en god ide at starte mødet med, at alle deltagere præsenterer sig med billede og lyd. Såfremt mødeformen ikke tillader det, bør deltagere præsentere sig med billede første gang de får ordet. På den måde kan man sikre, at der ikke er uvedkommende deltagere med til mødet.

A: God	B: Bedre	C: Bedst
Start mødet med, at alle deltagere præsenterer sig med billede og lyd. Alternativt bør deltagere præsentere sig med billede første gang de får ordet.	Brug en lobby funktion; luk først deltagere ind efter de er verificeret. Kun værten bør kunne styre hvem der lukkes ind til mødet og hvem der skal ekskluderes.	Se bedre.

Råd 6. Styring af hvem der kan præsentere lyd og billede
Uanset standardindstillinger for mødet, bør mødeleder altid kunne styre hvem, der kan tale og præsentere. Dette bidrager til at sikre, at mødet ikke undervejs uønsket kan overtages af andre deltagere.

En virtuel mødeplatform bør understøtte en standardkonfiguration for mødeindstillinger. Mødeplatformen bør som udgangspunkt være standardindstillet til, at kun værten kan præsentere, men har mulighed for at tildele andre mødedeltagere præsentationsrettigheder. Derudover er det en fordel, hvis der også kan laves standardindstillinger for mødetyper, fx webinarer, som er "én til mange"-møder eller arbejdsmøder, der typisk er "mange til mange"-møder. Det er en yderligere fordel, hvis det kan konfigureres, hvilke funktionaliteter deltagerne skal have til rådighed i det enkelte møde.

A: God	B: Bedre	C: Bedst
Værten kan styre mute/unmute lyd og præsentationer fra deltagere,	Konfigurér standardindstilling for møder, så kun værten kan styre mute/unmute lyd og præsentationer fra deltagere.	Konfigurér standardindstilling for møder. Granulær styring af hvem der kan mute/unmute lyd og tillade præsentationer fra deltagere. Valg af funktioner afhængig af mødetype.

Råd 7. Styring af lydoptagelser af møder
Nogle platforme giver mulighed for at optage mødet. Hvis der er en optagefunktion i applikationen, bør mødeværten kunne styre, om den er aktiv eller slået fra ved det pågældende møde. Værten kan dermed også styre, om det skal være muligt for deltagere at foretage en optagelse af mødet. Man skal være opmærksom på, at virtuelle møder pr. definition altid kan optages af den enkelte deltager med eget udstyr.

Hvis der optages fra et møde, er det vigtigt at være bevidst om formål samt ikke mindst den lovgivning, der gælder i forhold til de informationer, der behandles på mødet. Der kan eksempelvis være krav om kryptering og sletning i forhold til databeskyttelse og oplysningspligt til deltagerne om, at mødet optages.

A: God	B: Bedre	C: Bedst
Tilslutning af mødeoptagelse er synlig som minimum for værten.	Hvis platformen understøtter optagelse, skal det være muligt for værten at styre hvem, der kan benytte funktionen.	Granulær styring af hvem, der kan optage mødet. Optagelser gemmes krypteret og slettes automatisk efter et besluttet og angivet tidsrum.

Råd 8. Installér kun applikationer fra officielle tjenester
Malware, spionprogrammer og andre ondsindede applikationer kommer ofte via uofficielle distributionskanaler. Det bør så vidt muligt sikres, at møde-apps eller møde-add-ons til mobiltelefon, tablet eller computer, der kommer fra en ukendt tjeneste, eller som beder om ændringer sikkerhedsindstillingerne, ikke kan installeres.

Sørg for at it-afdelingen har en procedure for at hjælpe brugere, der skal deltage i virtuelle møder.

A: God	B: Bedre	C: Bedst
Installér kun apps fra officielle app-butikker eller producentens officielle hjemmeside.	It-afdelingen begrænser installation af apps til forhåndsgodkendte/whitelistede applikationer fra officielle app-butikker og eventuelt organisationens egen enterprise app-store.	Installation af applikationer sker via organisationens egen device management-løsning. Kun testede og godkendte apps kan installeres. Og det er kun it-afdelingen, som kan installere apps.

Valg af platform

Der bør altid ligge en risikobetragtning bag indkøb, implementering og brug af en it-løsning. Det gælder også for brug af virtuelle mødeplatforme.

For langt de fleste platforme er der tale om, at man køber et færdigt produkt, som man ikke har mulighed for at stille yderligere krav til. En "take it or leave it"-løsning. Der er ofte stor forskel på en gratis version og den version, man tilkøber som organisation. Betalingsversionerne udmærker sig ved, at have flere funktioner, større mulighed for kontrol og styring og dermed også bedre sikkerhed.

Ved afvejning af risici i forbindelse med anskaffelse bør organisationen i alle tilfælde stille sig selv en række spørgsmål, der kan være med til at give en pejling på, hvilken type platform og hvilken funktionalitet og styringsmulighed, man skal gå efter. Organisationen bør i særdeleshed forholde sig til, hvilke typer af informationer, der skal deles og arbejdes med via platformen. Den forventede brug er rammesættende for, om man skal lede efter en platform med kryptering, styringsmuligheder, muligheder for at slette data og profiler, etc.

Nogle centrale spørgsmål organisationen kan stille sig selv er:

- Hvad skal platformen bruges til? Har man brug for en platform, der hovedsageligt understøtter kommunikation via tekst og billede, eller har man brug for et reelt samarbejdsværktøj? Et pejlemærke er at jo mere funktionalitet – jo større behov for styring og kontrol.
- Hvor følsomme er de data, der skal deles/tales om på platformen? Et pejlemærke er, at hvis der skal deles sensitive data, skal platformen understøtte kryptering, og der bør anvendes strengere adgangskontrol.
- Er det vigtigt at holde styr på 3. parts adgang til og brug af data, herunder i forhold til GDPR-reglerne? Organisationen bør interessere sig for, om data på platformen opbevares lokalt, inden for EU eller uden for EU.
- Skal platformen udelukkende benyttes til lukkede interne møder, eller skal den bruges til samarbejde og kommunikation med eksterne, åbne konferencer etc.? Et pejlemærke er, at jo flere eksterne brugere – jo større behov for at kunne konfigurere platformen og tage styring på de enkelte funktioner
- Hvor mange brugere skal benytte platformen? Jo flere brugere – jo større afhængighed – jo større behov for driftssikker og gennemprøvet løsning.

Det kan være svært fuldstændigt at afdække evt. sårbarheder i en platform. Særligt fordi de hele tiden udvikles og opdateres. Derfor anbefaler Center for Cybersikkerhed, at man anvender internationalt anerkendte samarbejdsplatforme fra større leverandører, der gennem en længere periode positivt har påvist, at de håndterer sikkerhedsmæssige udfordringer.

Som hjælp til at vurdere de virtuelle mødeplatformes sikkerhed udgav USA's National Security Agency, NSA, i november 2020 en publikation med relevante kriterier, man som organisation med fordel kan læne sig op ad. NSA forholder sig til de mest gængse

virtuelle mødeplatforme på markedet, og publikationen kan med fordel læses i sin helhed. Herunder er gengivet en tabel fra publikationen, der giver et godt overblik over de enkelte produkter, holdt op imod kriterierne.

Særligt nyttigt er det, at tabellen giver et hurtigt overblik over, om kommunikation via platformen er end-to-end krypteret, om tilgang sker via flerfaktor-godkendelse, om der gives data videre til 3. part, om man har råderet – herunder sletteret over data – og om koden er offentlig tilgængelig og kan underkastes test.

For yderligere vejledning i forhold til valg af leverandør og brug af cloud-services, henvises i øvrigt til vejledning "Informationssikkerhed i Leverandørforhold" fra Center for Cybersikkerhed og Digitaliseringsstyrelsen og "Vejledning i anvendelse af cloudservices" fra Center for Cybersikkerhed og Digitaliseringsstyrelsen.

Table of Assessments against Criteria

Service	1 – End-to-End Encryption[5]					2 – Testable Encryption	3 – MFA	4 – Invitation Controls	5 – Minimal 3rd Party Sharing	6 – Secure Deletion	7 – Public Source Code Shared	8 – Certified Service (FedRAMP / NIAP
	Text Chat	Voice Calls	Video Calls	File Sharing	Screen Sharing							
Adobe Connect™ [i]	N	N	N	N	N	Y	Y	Y	Y	Client – Y Server – Y	N	FedRAMP
Amazon Chime™ [ii]	N	N	N	N	N	Y	Y	Y	N	Client – Y Server – Y	N	FedRAMP
Cisco Webex® [iii]	Y[1]	Y[1]	Y[1]	Y[1]	Y[1]	Y	Y[1, 2]	Y[1]	Y	Client – Y Server – N[3]	N	FedRAMP
Dust	Y	N/A	N/A	N/A	N/A	N[3]	N	Y	N	Client – Y Server – Y	N	None
Google Workspace™ [iv]	N	N	N	N	N	Y	Y[1]	Y[1, 4]	Y	Client – Y Server – Y[2]	N	FedRAMP
GoToMeeting® [v]	Y[1]	Y[1]	Y[1]	N/A	N/A	Y	N	Y[1]	Y	Client – Y Server – N[3]	N	None
Jitsi Meet® [vi]	Y[1]	Y[1]	Y[1]	Y[1]	Y[1]	Y	N	Y	N	Client – N[3] Server – N[3]	Y	None
Mattermost™ [vii]	N	N	N	N/A	N	Y	Y[2]	Y[4]	N	Client – Y Server – N	Y	None
Microsoft Teams® [viii]	N	N	N	N	N	Y	Y	Y	Y	Client – Y[1] Server – Y[1]	N	FedRAMP
Signal® [ix]	Y	Y	N/A	Y	N/A	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Skype for Business™ [x]	N	N	N	N	N	Y	Y	Y	Y	Client – Y[1] Server – Y[1]	N	FedRAMP
Slack® [xi]	N	N	N	N	N	Y	Y	Y	Y[1]	Client – Y_1 Server – Y_1	N	FedRAMP
SMS Text	N	N/A	N/A	N	N/A	N	N	N	N	Client – Y Server – N	N	None
WhatsApp® [xii]	Y	N/A	Y	Y	N/A	Y	Y	Y	Y	Client – Y Server – Y	N	None
Wickr® [xiii]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Wire	Y	Y	Y	Y	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Zoom® [xiv]	Y[1]	N	N	Y[1]	N	Y	Y[1]	Y	Y	Client – Y Server – N[3]	N	FedRAMP

Legend: Y = Yes, N = No; N/A = Not Applicable
1 Configurable
2 Free Version - N
3 No Published Details
4 Partial
5 End-to-end Encryption (E2EE) may be limited by app, browser, number of participants, or capabilities of other clients. Even without E2EE, all services (other than SMS) utilize link encryption between clients and servers whenever possible.

Kilde: NSA: Selecting and Safely Using Collaboration Services for Telework (se under referencer)

Ordforklaring til tabel

MFA – Multi Factor Authentification. Fler-faktor autentificering.

Secure deletion – produktet understøtter sikker sletning af data på henholdsvis klienten og serveren.

FedRAMP – Amerikansk organ der certificerer produkter op imod serien af NIST 800-53 standarder. NIST er en US standardiseringsorganisation og kan sammenlignes med CEN/CENELEC og til dels ISO. For bedre forståelse anbefales at læse NSA publikationen i sin helhed.

Referencer

CFCS: Cybersikkerhed ved hjemmearbejde:
https://cfcs.dk/da/temasider/distancearbejde/

CFCS og og Digitaliseringsstyrelsen: Informationssikkerhed i Leverandørforhold
https://cfcs.dk/da/forebyggelse/vejledninger/informationssikkerhed-i-leverandorforhold/

CFCS: Sikker brug af Transport Layer Security (TLS)
https://cfcs.dk/da/forebyggelse/vejledninger/tls/

Datatilsynet: Vejledende tekst om risikovurdering
https://www.datatilsynet.dk/Media/4/8/Risikovurdering.pdf

Digitaliseringsstyrelsen: Vejledning i anvendelse af cloudservices
https://digst.dk/data/vejledning-til-anvendelse-af-cloudservices/

ENISA: Tips for selecting and using online communication tools
https://www.enisa.europa.eu/news/enisa-news/tips-for-selecting-and-using-online-communication-tools

NSA: Selecting and Safely Using Collaboration Services for Telework
https://media.defense.gov/2020/Aug/14/2002477667/-1/-1/0/Collaboration_Services_UOO13459820_Full.PDF